TENT COOPERATION TRE. Y

From the INTERNATIONAL BUREAU

PCT

NOTIFICATION OF ELECTION

(PCT Rule 61.2)

To:

Commissioner
US Department of Commerce
United States Patent and Trademark Office, PCT
2011 South Clark Place Room CP2/5C24
Arlington, VA 22202
ETATS-UNIS D'AMERIQUE

in its capacity as elected Office

Date of mailing: 08 March 2001 (08.03.01)	
International application No.: PCT/JP00/05802	Applicant's or agent's file reference: 12577
International filing date: 28 August 2000 (28.08.00)	Priority date: 27 August 1999 (27.08.99)
Applicant: SHINDO, Jiro	

1. The designated Office is hereby notified of its election made:

[X] in the demand filed with the International preliminary Examining Authority on:

18 January 2001 (18.01.01)

[ ] in a notice effecting later election filed with the International Bureau on:

2. The election [X] was

[ ] was not

made before the expiration of 19 months from the priority date or, where Rule 32 applies, within the time limit under Rule 32.2(b).

The International Bureau of WIPO
34, chemin des Colombettes
1211 Geneva 20, Switzerland

Facsimile No.: (41-22) 740.14.35

Authorized officer:

J. Zahra

Telephone No.: (41-22) 338.83.38

Copy for the Elected Office (EO/US)

PCT/JP00/05802

PATENT COOPERATION TREATY

10/069,676

PCT

From the INTERNATIONAL BUREAU

To:

UMEDA, Akihiko
No.3 Seiko Building 7F
6-10, Akasaka 3-chome
Minato-ku, Tokyo 107-0052
JAPON

NOTIFICATION OF THE RECORDING OF A CHANGE

(PCT Rule 92bis.1 and Administrative Instructions, Section 422)

Date of mailing (day/month/year) 11 March 2002 (11.03.02)	
Applicant's or agent's file reference 12577	**IMPORTANT NOTIFICATION**
International application No. PCT/JP00/05802	**International filing date** (day/month/year) 28 August 2000 (28.08.00)

1. The following indications appeared on record concerning:

[X] the applicant [ ] the inventor [ ] the agent [ ] the common representative

Name and Address	State of Nationality	State of Residence
DIGITAL PUBLISHING JAPAN CO. LTD. 196-1, Kamigamo-Motoyama, Kita-ku Kyoto-shi, Kyoto 603-8047 Japan	JP	JP
	Telephone No.	
	Facsimile No.	
	Teleprinter No.	

2. The International Bureau hereby notifies the applicant that the following change has been recorded concerning:

[ ] the person [X] the name [ ] the address [ ] the nationality [ ] the residence

Name and Address	State of Nationality	State of Residence
Celartem Technology Inc. 196-1, Kamigamo-Motoyama, Kita-ku Kyoto-shi, Kyoto 603-8047 Japan	JP	JP
	Telephone No.	
	Facsimile No.	
	Teleprinter No.	

3. Further observations, if necessary:

4. A copy of this notification has been sent to:

[X] the receiving Office
[ ] the International Searching Authority
[ ] the International Preliminary Examining Authority
[ ] the designated Offices concerned
[X] the elected Offices concerned
[ ] other:

The International Bureau of WIPO **34, chemin des Colombettes** **1211 Geneva 20, Switzerland**	Authorized officer Akiko KOYAMA
Facsimile No.: (41-22) 740.14.35	Telephone No.: (41-22) 338.83.38

004713273

Form PCT/IB/306 (March 1994)

Copy for the Elected Office (EO/US)

PCT/JP00/05802

PATENT COOPERATION TREATY

From the INTERNATIONAL BUREAU

PCT

NOTIFICATION OF THE RECORDING OF A CHANGE

(PCT Rule 92bis.1 and Administrative Instructions, Section 422)

To:

UMEDA, Akihiko
No.3 Seiko Building 7F
6-10, Akasaka 3-chome
Minato-ku, Tokyo 107-0052
JAPON

Date of mailing (day/month/year)
11 March 2002 (11.03.02)

Applicant's or agent's file reference
12577

IMPORTANT NOTIFICATION

International application No.
PCT/JP00/05802

International filing date (day/month/year)
28 August 2000 (28.08.00)

1. The following indications appeared on record concerning:

[X] the applicant [X] the inventor [ ] the agent [ ] the common representative

Name and Address
SHINDO, Jiro
Digital Publishing Japan Co. Ltd.
196-1, Kamigamo-Motoyama, Kita-ku
Kyoto-shi, Kyoto 603-8047
Japan

State of Nationality: JP
State of Residence: JP
Telephone No.:
Facsimile No.:
Teleprinter No.:

2. The International Bureau hereby notifies the applicant that the following change has been recorded concerning:

[ ] the person [ ] the name [X] the address [ ] the nationality [ ] the residence

Name and Address
SHINDO, Jiro
Celartem Technology Inc.
196-1, Kamigamo-Motoyama
Kita-ku
Kyoto-shi
Kyoto 603-8047
Japan

State of Nationality: JP
State of Residence: JP
Telephone No.:
Facsimile No.:
Teleprinter No.:

3. Further observations, if necessary:

4. A copy of this notification has been sent to:

[X] the receiving Office
[ ] the International Searching Authority
[ ] the International Preliminary Examining Authority
[ ] the designated Offices concerned
[X] the elected Offices concerned
[ ] other:

The International Bureau of WIPO
34, chemin des Colombettes
1211 Geneva 20, Switzerland

Facsimile No.: (41-22) 740.14.35

Authorized officer
Akiko KOYAMA

Telephone No.: (41-22) 338.83.38

Form PCT/IB/306 (March 1994)

004713274

10/069676

Translation

PATENT COOPERATION TREATY

PCT

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

(PCT Article 36 and Rule 70)

Applicant's or agent's file reference 12577	FOR FURTHER ACTION	See Notification of Transmittal of International Preliminary Examination Report (Form PCT/IPEA/416)
International application No. PCT/JP00/05802	International filing date (*day/month/year*) 28 August 2000 (28.08.00)	Priority date (*day/month/year*) 27 August 1999 (27.08.99)
International Patent Classification (IPC) or national classification and IPC H04N 1/387, G06F 12/14, 15/00, G06T 1/00		
Applicant DIGITAL PUBLISHING JAPAN CO. LTD.		

1. This international preliminary examination report has been prepared by this International Preliminary Examining Authority and is transmitted to the applicant according to Article 36.

2. This REPORT consists of a total of 3 sheets, including this cover sheet.

☒ This report is also accompanied by ANNEXES, i.e., sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications made before this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions under the PCT).

These annexes consist of a total of 6 sheets.

3. This report contains indications relating to the following items:

- I ☒ Basis of the report
- II ☐ Priority
- III ☐ Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- IV ☐ Lack of unity of invention
- V ☒ Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
- VI ☐ Certain documents cited
- VII ☐ Certain defects in the international application
- VIII ☐ Certain observations on the international application

Date of submission of the demand 18 January 2001 (18.01.01)	Date of completion of this report 16 October 2001 (16.10.2001)
Name and mailing address of the IPEA/JP Facsimile No.	Authorized officer Telephone No.

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.
PCT/JP00/05802

I. Basis of the report

1. With regard to the **elements** of the international application:*

☐ the international application as originally filed

☒ the description:

pages 1-10, as originally filed

pages _____, filed with the demand

pages _____, filed with the letter of _____

☒ the claims:

pages 1-5,9,17,24, as originally filed

pages _____, as amended (together with any statement under Article 19

pages _____, filed with the demand

pages 25-49, filed with the letter of 28 September 2001 (28.09.2001)

☒ the drawings:

pages 1,2, as originally filed

pages _____, filed with the demand

pages _____, filed with the letter of _____

☐ the sequence listing part of the description:

pages _____, as originally filed

pages _____, filed with the demand

pages _____, filed with the letter of _____

2. With regard to the **language**, all the elements marked above were available or furnished to this Authority in the language in which the international application was filed, unless otherwise indicated under this item.
These elements were available or furnished to this Authority in the following language _____ which is:

☐ the language of a translation furnished for the purposes of international search (under Rule 23.1(b)).

☐ the language of publication of the international application (under Rule 48.3(b)).

☐ the language of the translation furnished for the purposes of international preliminary examination (under Rule 55.2 and/or 55.3).

3. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, the international preliminary examination was carried out on the basis of the sequence listing:

☐ contained in the international application in written form.

☐ filed together with the international application in computer readable form.

☐ furnished subsequently to this Authority in written form.

☐ furnished subsequently to this Authority in computer readable form.

☐ The statement that the subsequently furnished written sequence listing does not go beyond the disclosure in the international application as filed has been furnished.

☐ The statement that the information recorded in computer readable form is identical to the written sequence listing has been furnished.

4. ☒ The amendments have resulted in the cancellation of:

☐ the description, pages _____

☒ the claims, Nos. 6-8,10-16,18-23

☐ the drawings, sheets/fig _____

5. ☐ This report has been established as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed, as indicated in the Supplemental Box (Rule 70:2(c)).**

* *Replacement sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to this report since they do not contain amendments (Rule 70.16 and 70.17).*

** *Any replacement sheet containing such amendments must be referred to under item 1 and annexed to this report.*

V. Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Claims	4-5,9,17,24-29	YES
	Claims	1-3	NO
Inventive step (IS)	Claims	17,41-49	YES
	Claims	1-5,9,24-40	NO
Industrial applicability (IA)	Claims	1-5,9,17,24-49	YES
	Claims		NO

2. Citations and explanations

Claims 1-3, 5, 9, 25-38 and 40
Document 1: JP, 11-66010, A (Canon Inc.), 9 March, 1999 (09.03.99), full text, Figs. 1-12
Document 2: JP, 11-212461, A (Canon Inc.), 6 August, 1999 (06.08.99), full text, Figs. 1-17
Document 3: JP, 11-69137, A (Canon Inc.), 9 March, 1999 (09.03.99), full text, Figs. 1-12
Document 4: JP, 11-232264, A (Canon Inc.), 27 August, 1999 (27.08.99), full text, Figs. 1-8

The above documents describe the image distribution technique of adding a user's security data as an electronic watermark to image data (by the client side according to documents 1 and 2) in order to prevent illegal use of the image data by its distribution from the server side to the client side via a network and so the subject matters of claim 1-3 do not appear to be novel.

The technique of transmitting an electronic key to open image data as described in claims 5-9, the technique of adding the quality of resolution or size of an image in a client's request as described in claims 25-27 and 31-33, the technique of storing a communication status between the server side and the security side as described in claims 28 and 35, and the technique of providing the IP address of a security controller or the like as described in claims 29, 36 and 40 are considered to be commonly-known art ordinarily used in the technical field concerned, and the subject matters of claims 5, 9, 25-38 and 40 could have been easily conceived of based on the inventions disclosed in the above documents 1-4.

Claims 4, 24 and 39
Documents 5: JP, 11-69134, A (Sony Corporation), 9 March, 1999 (09.03.99), full text, Figs. 1-13
Documents 6: JP, 9-252397, A (Tateba System K.K.), 22 September, 1997 (22.09.97), full text, Figs. 1-3

The above documents describe the technique of adjusting the brightness of selected pixels when information is added to image data, and so applying the said technique to the inventions of documents 1-4 could have been easily conceived of.

Claims 17 and 41-49
Document 7: JP, 11-203075, A (Canon, Inc.), 30 July, 1999 (30.07.99), full text, Figs. 1-5

The above document defining the general state of the art in the technical field concerned, the technique of allowing access between a security control server and a client for authenticating the acquisition of image data is neither described nor suggested in any of documents 1-7.

EP・US　　特許協力条約

PCT

国際調査報告

（法８条、法施行規則第40、41条）
〔ＰＣＴ１８条、ＰＣＴ規則43、44〕

出願人又は代理人の書類記号　１２５７７	今後の手続きについては、国際調査報告の送付通知様式（ＰＣＴ／ＩＳＡ／２２０）及び下記５を参照すること。	
国際出願番号 ＰＣＴ／ＪＰ００／０５８０２	国際出願日（日.月.年）　２８．０８．００	優先日（日.月.年）　２７．０８．９９
出願人（氏名又は名称）　株式会社デジタル・パブリッシング・ジャパン		

国際調査機関が作成したこの国際調査報告を法施行規則第41条（ＰＣＴ１８条）の規定に従い出願人に送付する。
この写しは国際事務局にも送付される。

この国際調査報告は、全部で　3　ページである。

☐ この調査報告に引用された先行技術文献の写しも添付されている。

１．国際調査報告の基礎

ａ．言語は、下記に示す場合を除くほか、この国際出願がされたものに基づき国際調査を行った。
- ☐ この国際調査機関に提出された国際出願の翻訳文に基づき国際調査を行った。

ｂ．この国際出願は、ヌクレオチド又はアミノ酸配列を含んでおり、次の配列表に基づき国際調査を行った。
- ☐ この国際出願に含まれる書面による配列表
- ☐ この国際出願と共に提出されたフレキシブルディスクによる配列表
- ☐ 出願後に、この国際調査機関に提出された書面による配列表
- ☐ 出願後に、この国際調査機関に提出されたフレキシブルディスクによる配列表
- ☐ 出願後に提出した書面による配列表が出願時における国際出願の開示の範囲を超える事項を含まない旨の陳述書の提出があった。
- ☐ 書面による配列表に記載した配列とフレキシブルディスクによる配列表に記録した配列が同一である旨の陳述書の提出があった。

２．☐ 請求の範囲の一部の調査ができない（第Ｉ欄参照）。

３．☐ 発明の単一性が欠如している（第Ⅱ欄参照）。

４．発明の名称は
- ☒ 出願人が提出したものを承認する。
- ☐ 次に示すように国際調査機関が作成した。

５．要約は
- ☒ 出願人が提出したものを承認する。
- ☐ 第Ⅲ欄に示されているように、法施行規則第47条（ＰＣＴ規則38.2(b)）の規定により国際調査機関が作成した。出願人は、この国際調査報告の発送の日から１カ月以内にこの国際調査機関に意見を提出することができる。

６．要約書とともに公表される図は、第　1　図とする。
- ☒ 出願人が示したとおりである。
- ☐ 出願人は図を示さなかった。
- ☐ 本図は発明の特徴を一層よく表している。
- ☐ なし

国際調[redacted]告　　国際出[redacted]号　PCT／JP00／05802

A.　発明の属する分野の分類（国際特許分類（IPC））

Int. Cl'　H04N1／387, G06F12／14, G06F15／00, G06T1／00

B.　調査を行った分野

調査を行った最小限資料（国際特許分類（IPC））

Int. Cl'　H04N1／38－1／393, G06F12／14, G06F15／00

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	1922－1996年
日本国公開実用新案公報	1971－2000年
日本国登録実用新案公報	1994－2000年
日本国実用新案登録公報	1996－2000年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

C.　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
	JP, 11－66010, A（キヤノン株式会社） 9. 3月. 1999（09. 03. 99）	
X	全文, 第1－12図	1-3, 5-14, 16
Y	全文, 第1－12図 & EP, 898396, A2	4, 15, 24
	JP, 11－212461, A（キヤノン株式会社） 6. 8月. 1999（06. 08. 99）	
X	全文, 第1－17図	1-3, 5-14, 16
Y	全文, 第1－17図（ファミリーなし）	4, 15, 24

☒ C欄の続きにも文献が列挙されている。　☐ パテントファミリーに関する別紙を参照。

＊　引用文献のカテゴリー
「A」特に関連のある文献ではなく、一般的技術水準を示すもの
「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「O」口頭による開示、使用、展示等に言及する文献
「P」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献
「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Y」特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「&」同一パテントファミリー文献

国際調査を完了した日　12. 12. 00	国際調査報告の発送日　26.12.00
国際調査機関の名称及びあて先 日本国特許庁（ISA／JP） 郵便番号100－8915 東京都千代田区霞が関三丁目4番3号	特許庁審査官（権限のある職員）　5V　9067 橋爪　正樹 電話番号　03－3581－1101　内線　3571

様式PCT／ISA／210（第2ページ）（1998年7月）

C（続き）．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
	JP，11－69137，A（キヤノン株式会社） 9．3月．1999（09．03．99）	
X	全文，第1－12図	1-3, 5-14, 16
Y	全文，第1－12図 ＆ EP，898396，A2	4, 15, 24
	JP，11－234264，A（キヤノン株式会社） 27．8月．1999（27．08．99）	
X	全文，第1－8図	1-3, 5-14, 16
Y	全文，第1－8図 （ファミリーなし）	4, 15, 24
Y	JP，11－69134，A（ソニー株式会社） 9．3月．1999（09．03．99） 全文，第1－13図（ファミリーなし）	4, 15, 24
Y	JP，9－252397，A（立羽システム株式会社） 22．9月．1997（22．09．97） 全文，第1－3図（ファミリーなし）	4, 15, 24
A	JP，10－191036，A（株式会社モノリス） 21．7月．1998（21．07．98） 全文，第1－16図 ＆ WO，98／20672，A2 ＆ AU，5430898，A ＆ EP，938807，A	1－24
A	JP，10－285381，A（松下電送システム株式会社） 23．10月．1998（23．10．98） 全文，第1－4図（ファミリーなし）	1－24
A	JP，11－203075，A（キヤノン株式会社） 30．7月．1999（30．07．99） 全文，第1－5図（ファミリーなし）	1－24

PCT

特許協力条約

国際予備審査報告

（法第１２条、法施行規則第56条）
〔ＰＣＴ３６条及びＰＣＴ規則70〕

出願人又は代理人の書類記号　１２５７７	今後の手続きについては、国際予備審査報告の送付通知（様式ＰＣＴ／ＩＰＥＡ／４１６）を参照すること。	
国際出願番号 ＰＣＴ／ＪＰ００／０５８０２	国際出願日（日.月.年）　２８．０８．００	優先日（日.月.年）　２７．０８．９９
国際特許分類（ＩＰＣ） Ｉｎｔ．Ｃｌ' Ｈ０４Ｎ１／３８７，Ｇ０６Ｆ１２／１４，Ｇ０６Ｆ１５／００，Ｇ０６Ｔ１／００		
出願人（氏名又は名称） 株式会社デジタル・パブリッシング・ジャパン		

1．　国際予備審査機関が作成したこの国際予備審査報告を法施行規則第57条（ＰＣＴ３６条）の規定に従い送付する。

2．　この国際予備審査報告は、この表紙を含めて全部で　4　ページからなる。

☒ この国際予備審査報告には、附属書類、つまり補正されて、この報告の基礎とされた及び／又はこの国際予備審査機関に対してした訂正を含む明細書、請求の範囲及び／又は図面も添付されている。
（ＰＣＴ規則70.16及びＰＣＴ実施細則第６０７号参照）
この附属書類は、全部で　6　ページである。

3．　この国際予備審査報告は、次の内容を含む。

- Ⅰ ☒ 国際予備審査報告の基礎
- Ⅱ ☐ 優先権
- Ⅲ ☐ 新規性、進歩性又は産業上の利用可能性についての国際予備審査報告の不作成
- Ⅳ ☐ 発明の単一性の欠如
- Ⅴ ☒ ＰＣＴ３５条(2)に規定する新規性、進歩性又は産業上の利用可能性についての見解、それを裏付けるための文献及び説明
- Ⅵ ☐ ある種の引用文献
- Ⅶ ☐ 国際出願の不備
- Ⅷ ☐ 国際出願に対する意見

国際予備審査の請求書を受理した日　１８．０１．０１	国際予備審査報告を作成した日　１６．１０．０１
名称及びあて先 日本国特許庁（ＩＰＥＡ／ＪＰ） 郵便番号１００－８９１５ 東京都千代田区霞が関三丁目４番３号	特許庁審査官（権限のある職員）　５Ｖ　９０６７ 橋爪　正樹 電話番号　０３－３５８１－１１０１　内線　３５７１

様式ＰＣＴ／ＩＰＥＡ／４０９（表紙）（１９９８年７月）

国際予備審査報告　　国際出願番号　ＰＣＴ／ＪＰ００／０５８０２

Ⅰ．　国際予備審査報告の基礎

1．　この国際予備審査報告は下記の出願書類に基づいて作成された。（法第６条（ＰＣＴ１４条）の規定に基づく命令に応答するために提出された差し替え用紙は、この報告書において「出願時」とし、本報告書には添付しない。ＰＣＴ規則70.16, 70.17）

☐ 出願時の国際出願書類

☒ 明細書　第　１－１０　ページ、　出願時に提出されたもの
明細書　第　　ページ、　国際予備審査の請求書と共に提出されたもの
明細書　第　　ページ、　　付の書簡と共に提出されたもの

☒ 請求の範囲　第　１－５，９，１７，２４　項、　出願時に提出されたもの
請求の範囲　第　　項、　ＰＣＴ１９条の規定に基づき補正されたもの
請求の範囲　第　　項、　国際予備審査の請求書と共に提出されたもの
請求の範囲　第　２５－４９　項、　２８．０９．０１　付の書簡と共に提出されたもの

☒ 図面　第　１，２　~~ページ／~~図、　出願時に提出されたもの
図面　第　　ページ／図、　国際予備審査の請求書と共に提出されたもの
図面　第　　ページ／図、　　付の書簡と共に提出されたもの

☐ 明細書の配列表の部分　第　　ページ、　出願時に提出されたもの
明細書の配列表の部分　第　　ページ、　国際予備審査の請求書と共に提出されたもの
明細書の配列表の部分　第　　ページ、　　付の書簡と共に提出されたもの

2．　上記の出願書類の言語は、下記に示す場合を除くほか、この国際出願の言語である。

上記の書類は、下記の言語である　　語である。

☐ 国際調査のために提出されたＰＣＴ規則23.1(b)にいう翻訳文の言語
☐ ＰＣＴ規則48.3(b)にいう国際公開の言語
☐ 国際予備審査のために提出されたＰＣＴ規則55.2または55.3にいう翻訳文の言語

3．　この国際出願は、ヌクレオチド又はアミノ酸配列を含んでおり、次の配列表に基づき国際予備審査報告を行った。

☐ この国際出願に含まれる書面による配列表
☐ この国際出願と共に提出されたフレキシブルディスクによる配列表
☐ 出願後に、この国際予備審査（または調査）機関に提出された書面による配列表
☐ 出願後に、この国際予備審査（または調査）機関に提出されたフレキシブルディスクによる配列表
☐ 出願後に提出した書面による配列表が出願時における国際出願の開示の範囲を超える事項を含まない旨の陳述書の提出があった
☐ 書面による配列表に記載した配列とフレキシブルディスクによる配列表に記録した配列が同一である旨の陳述書の提出があった。

4．　補正により、下記の書類が削除された。
☐ 明細書　第　　ページ
☒ 請求の範囲　第　6-8, 10-16, 18-23　項
☐ 図面　図面の第　　ページ／図

5．☐ この国際予備審査報告は、補充欄に示したように、補正が出願時における開示の範囲を越えてされたものと認められるので、その補正がされなかったものとして作成した。（ＰＣＴ規則70.2(c)　この補正を含む差し替え用紙は上記１．における判断の際に考慮しなければならず、本報告に添付する。）

Ⅴ．　新規性、進歩性又は産業上の利用可能性についての法第１２条（ＰＣＴ３５条(2)）に定める見解、それを裏付ける文献及び説明

１．　見解

新規性（N）	請求の範囲	４－５，９，１７，２４－４９	有
	請求の範囲	１－３	無
進歩性（ＩＳ）	請求の範囲	１７，４１－４９	有
	請求の範囲	１－５，９，２４－４０	無
産業上の利用可能性（ＩＡ）	請求の範囲	１－５，９，１７，２４－４９	有
	請求の範囲		無

２．　文献及び説明（ＰＣＴ規則70.7）

請求の範囲１－３，５，９，２５－３８，４０

文献１：ＪＰ　１１－６６０１０　Ａ（キヤノン株式会社）
９．３月．１９９９（０９．０３．９９）全文，第１－１２図
文献２：ＪＰ　１１－２１２４６１　Ａ（キヤノン株式会社）
６．８月．１９９９（０６．０８．９９）全文，第１－１７図
文献３：ＪＰ　１１－６９１３７　Ａ（キヤノン株式会社）
９．３月．１９９９（０９．０３．９９）全文，第１－１２図
文献４：ＪＰ　１１－２３２２６４　Ａ（キヤノン株式会社）
２７．８月．１９９９（２７．０８．９９）全文，第１－８図

には、サーバ側からネットワークを介してクライアント側への画像データの配信を行うに際し、画像データの不正使用を防止するために、（文献１及び２においてはクライアント側において）前記画像データに対してユーザのセキュリティデータを電子透かしとして付加する画像データ配信技術が記載されており、請求の範囲１－３に係る発明に関しては新規性を有しない。

また、請求の範囲５及び９に記載されているような、画像データを開くための電子キーを送信する技術、請求の範囲２５－２７，３１－３３に記載されているような、クライアントからの要求の中に画像の解像度又はサイズに関する品質を含める技術、請求の範囲２８，３５に記載されているような、サーバ側とセキュリティ側との通信状況を保存する技術、及び請求の範囲２９，３６、４０に記載されているような、セキュリティコントローラ等のＩＰアドレスを付与する技術は、当該技術分野において通常よく使われている周知技術にすぎないと認められ、請求の範囲５，９、２５－３８，４０に係る発明は、上記文献１－４に記載された発明に基づいて、当業者が容易に想到し得る発明にすぎない。

請求の範囲４，２４，３９

文献５：ＪＰ　１１－６９１３４　Ａ（ソニー株式会社）
９．３月．１９９９（０９．０３．９９）全文，第１－１３図
文献６：ＪＰ　９－２５２３９７　Ａ（立羽システム株式会社）
２２．９月．１９９７（２２．０９．９７）全文，第１－３図

には、画像データに対する情報の付加において、選択した画素の輝度を調節する技術が記載されており、文献１－４に記載された発明に対して当該技術を適用することに格別の困難性があるとは認められない。

補充欄（いずれかの欄の大きさが足りない場合に使用すること）

第　V　欄の続き

請求の範囲１７，４１－４９
文献７：ＪＰ　１１－２０３０７５　Ａ（キヤノン株式会社）
３０．７月．１９９９（３０．０７．９９）全文，第１－５図
は、当該技術分野における一般的技術水準を示す文献であって、セキュリテイコントロールサーバとクライアントとの間で画像データ取得の認証の付与に関してアクセスを行う技術に関しては、文献１－７のいずれにも記載も示唆もされていない。

請求の範囲

1．サーバ側からネットワークを介してクライアント側への画像データの配信において画像データの不正使用を防止するために、前記クライアント側において、前記サーバ側から配信された画像データをメモリ上に展開した後、展開した前記画像データにユーザのセキュリティデータを付加する過程とを含むことを特徴とする画像データ配信方法。

2．前記クライアント側から前記サーバ側に前記ユーザのセキュリティデータを送信する過程と、前記セキュリティデータを前記サーバ側の記憶装置に保存させる過程とを更に含むことを特徴とする請求項1に記載の画像データ配信方法。

3．前記セキュリティデータを電子透かしとして前記画像データに付加することを特徴とする請求項1又は2のいずれかに記載の画像データ配信方法。

4．メモリ上に展開した前記画像データの各画素の中で連続しない位置にある複数の画素を選択し、選択した前記画素の輝度を増加又は減少させることにより、前記セキュリティデータを前記画像データに付加することを特徴とする請求項1乃至3のいずれかに記載の画像データ配信方法。

5．サーバ側からネットワークを介してクライアント側への画像データの配信において画像データの不正使用を防止するために、前記サーバ側において、クライアントからの要求に応答して、画像データ配信の認証を行うセキュリティコントローラへのアクセスを前記クライアント側に指示する過程と、前記クライアント側からの画像データ配信の認証要求に応答して、前記セキュリティコントローラから前記クライアント側に、画像データを開くための電子キーを送信する過程とを含むことを特徴とする画像データ配信方法。

6．（削除）

7．（削除）

8．（削除）

9．サーバからクライアントへ画像データを配信するための方法であって、

クライアント側からの画像データの要求に応答して、サーバ側から前記クライアント側にセキュリティコントローラへのアクセスを指示する過程と、

前記クライアント側から前記セキュリティコントローラにアクセスして、画像データ配信の認証を求める過程と、

前記サーバ側から前記クライアント側に前記要求に対応した画像データを送信する過程と、

前記サーバ側から前記クライアント側に前記画像データを開くための画像キーを送信する過程と、

前記クライアント側において、前記画像キーを用いて前記画像データを開き、該画像データにユーザ又はクライアントのセキュリティデータを付加する過程と、

前記セキュリティデータを付加した画像データを出力する過程とからなることを特徴とする画像データ配信方法。

１０．（削除）

１１．（削除）

１２．（削除）

１３．（削除）

１４．（削除）

１５．（削除）

１６．（削除）

１７．画像ファイルを蓄積した画像ファイルデータベースを有する画像ファイルサーバと、

各ユーザの登録データを蓄積したユーザデータベースと、前記各画像ファイルを開くための画像キーを蓄積した画像キーデータベースとを有するセキュリティコントロールサーバと、

クライアントと、

前記画像ファイルサーバ、前記セキュリティコントロールサーバ及び前記クライアントを接続するネットワークとを備え、

前記画像ファイルサーバが、前記クライアントからの画像データの要求に応答して、前記クライアントに前記セキュリティコントロールサーバへのアクセスを指示する機能と、要求された画像データを前記クライアントに送信する機能とを

有し、

前記クライアントが、前記セキュリティコントロールサーバにアクセスして、ユーザの前記画像データ取得の認証を要求する機能を有し、

前記セキュリティコントロールサーバが、前記クライアントからの認証の要求に応答して、前記ユーザデータベースを確認して前記ユーザに認証を付与し、前記画像キーデータベースから前記要求された画像データの画像キーを送信する機能を有し、

前記クライアントが更に、前記画像キーを用いて、受信した前記画像データを開き、かつ前記画像データに前記ユーザのセキュリティデータを付加する機能を有することを特徴とする画像データ配信システム。

１８．（削除）

１９．（削除）

２０．（削除）

２１．（削除）

２２．（削除）

２３．（削除）

２４．各ドットの画素データのマップからなり、その位置が連続していない複数の選択した画素について、その輝度を増加又は減少させることにより、ユーザの情報を埋め込んだことを特徴とする画像データ。

２５．（追加）前記画像データが画像の品質の異なる画像ファイルを有し、前記クライアントからの要求が画像の品質の指定を含むことを特徴とする請求項５に記載の画像データ配信方法。

２６．（追加）前記画像データが、画像の品質によって階層化されたデータ構造の画像ファイルを有することを特徴とする請求項２５に記載の画像データ配信方法。

２７．（追加）前記画像の品質が画像の解像度又はサイズであることを特徴とする請求項２５又は２６に記載の画像データ配信方法。

２８．（追加）前記クライアント側との通信状況を保存する過程を更に含むことを特徴とする請求項５、２５乃至２７のいずれかに記載の画像データ配信方法。

２９．（追加）前記セキュリティコントローラのＩＰアドレスを付与することにより、前記セキュリティコントローラへのアクセスを指示することを特徴とする請求項５、２５乃至２８のいずれかに記載の画像データ配信方法。

３０．（追加）請求項１乃至３、５、２５乃至２９のいずれかに記載の画像データ配信方法を実行するためのソフトウエアを記憶した記録媒体。

３１．（追加）前記画像データが画像の品質の異なる画像ファイルを有し、前記クライアントからの要求が画像の品質の指定を含むことを特徴とする請求項９に記載の画像データ配信方法。

３２．（追加）前記画像データが、画像の品質によって階層化されたデータ構造の画像ファイルを有することを特徴とする請求項３１に記載の画像データ配信方法。

３３．（追加）前記画像の品質が画像の解像度又はサイズであることを特徴とする請求項３１又は３２に記載の画像データ配信方法。

３４．（追加）前記セキュリティデータを前記サーバ側に送信する過程と、該セキュリティデータを前記サーバ側において保存する過程とを更に含むことを特徴とする請求項９、３１乃至３３のいずれかに記載の画像データ配信方法。

３５．（追加）前記サーバ側において前記クライアント側との通信状況をログファイルに保存する過程を更に有することを特徴とする請求項９、３１乃至３４のいずれかに記載の画像データ配信方法。

３６．（追加）前記セキュリティコントローラのＩＰアドレスを付与することにより、前記セキュリティコントローラへのアクセスを指示することを特徴とする請求項９、３１乃至３５のいずれかに記載の画像データ配信方法。

３７．（追加）前記サーバ側から送信される前記画像データが圧縮されており、該画像データを前記クライアント側において解凍した後に、前記セキュリティデータを付加することを特徴とする請求項９、３１乃至３６のいずれかに記載の画像データ配信方法。

３８．（追加）前記セキュリティデータを電子透かしとして前記画像データに付加することを特徴とする請求項９、３１乃至３７のいずれかに記載の画像データ配信方法。

３９．（追加）前記画像キーを用いて開いた前記画像データの各画素の中で連続しない位置にある複数の画素を選択し、選択した前記画素の輝度を増加又は減少させることにより、前記セキュリティデータを前記画像データに付加することを特徴とする請求項９、３１乃至３８のいずれかに記載の画像データ配信方法。

４０．（追加）前記セキュリティデータには、前記画像データの配信日時、ユーザＩＤ、前記画像データを保存した前記クライアントの記憶装置のシリアル番号、又は前記クライアントのＩＰアドレスが含まれることを特徴とする請求項９、３１乃至３９のいずれかに記載の画像データ配信方法。

４１．（追加）前記画像データが画像の品質の異なる画像ファイルを有し、前記クライアントからの要求が画像の品質の指定を含むことを特徴とする請求項１７に記載の画像データ配信システム。

４２．（追加）前記画像データが、画像の品質によって階層化されたデータ構造の画像ファイルを有することを特徴とする請求項４１に記載の画像データ配信システム。

４３．（追加）前記画像の品質が画像の解像度又はサイズであることを特徴とする請求項４１又は４２に記載の画像データ配信システム。

４４．（追加）前記クライアントが、前記セキュリティデータを前記セキュリティコントロールサーバに送信する機能を更に有し、前記セキュリティコントロールサーバが、前記セキュリティデータを保存する機能を更に有することを特徴とする請求項１７、４１乃至４３のいずれかに記載の画像データ配信システム。

４５．（追加）前記セキュリティコントロールサーバが、前記クライアントとの通信状況を保存するためのログファイルを有することを特徴とする請求項１７、４１乃至４４のいずれかに記載の画像データ配信システム。

４６．（追加）前記画像ファイルサーバが、前記セキュリティコントロールサーバのＩＰアドレスを付与することにより、それへのアクセスを指示することを特徴とする請求項１７、４１乃至４５のいずれかに記載の画像データ配信システム。

４７．（追加）前記画像ファイルサーバから送信される前記画像データが圧縮されており、前記クライアントが、受信した前記画像データを解凍し、かつその後

に前記セキュリティデータを付加することを特徴とする請求項１７、４１乃至４６のいずれかに記載の画像データ配信システム。

４８．（追加）前記クライアントが、前記セキュリティデータを電子透かしとして前記画像データに付加する機能を有することを特徴とする請求項１７、４１乃至４７のいずれかに記載の画像データ配信システム。

４９．（追加）前記セキュリティデータには、前記画像データの配信日時、ユーザＩＤ、前記画像データを保存した前記クライアントの記憶装置のシリアル番号、又は前記クライアントのＩＰアドレスが含まれることを特徴とする請求項１７、４１乃至４８のいずれかに記載の画像データ配信システム。

Procedure Amendments

(Amendments according to the provision of Article 11 of the Law)

To: Patent Office examiner

1. Indication of international application: PCT/JP00/05802
2. Applicant:

   Name: Digital Publishing Japan Co., Ltd.

   Address: 196-1 Kamigamo-Motoyama, Kita-ku, Kyoto-shi, Kyoto-fu, 603-8047, Japan

   Nationality: Japan

   Address: Japan
3. Agent:

   Name: (9806) patent attorney, Akihiko Umeda

   Address: No. 3 Seiko Building 7F, 3-6-10 Akasaka, Minato-ku, Tokyo-to, 107-0052, Japan
4. Item to be amended: Claims
5. Amendment contents:

   (1) Claims 6-8 of pages 11 and 12, Claims 10-16 of pages 12 and 13, and Claims 18-23 of page 14 are deleted.

   (2) Claims 25-49 are added.
6. List of attached documents

   (1) Pages 11-14 and 14/1-14/2 of the claims

[recurring header:] [pages 1-3 of 3]

International Application Form in accordance with Patent Cooperation Treaty

Original copy (for application) – Time and date printed August 28, 2000 (08.28.2000) Monday 16 h. 24 min. 15 sec.

0. For use by accepting agency

0-1 International Application No.

0-2 International Filing Date

0-3 (acceptance stamp)

0-4 Format–PCT/R0/101

This international application form in accordance with Patent Cooperation Treaty was

0-4-1 Prepared according to the right: PCT-EASY Version 2.91 (updated 07.01.2000)

0-5 Instance

Applicant requests that this international application be processed in accordance with Patent Cooperation Treaty.

0-6 Accepting agency designated by applicant: Patent Office of Japan (RO/JP)

0-7 Document symbol of applicant or agent: 12577

I Title of the invention:

Image data distribution method and system, image data and storage medium

II Applicant

II-1 Party entered in this column is: Applicant only

II-2 Applicant applicable to the countries designated on the right:

All designated countries states except US

II-4ja Name: K.K. Digital Publishing Japan

II-4en Digital Publishing Japan Co., Ltd.

II-5ja Address: 196-1 Kamigamohonzan, Kita-ku, Kyoto-shi, Kyoto 603-8047, Japan

II-5en 196-1 Kamigamohonzan, Kita-ku, Kyoto-shi, Kyoto 603-8047, Japan

II-6 Nationality (Name of country): Japan JP

II-7 Address (Name of country): Japan JP

II-8 Telephone No.: 075-712-5161

II-9 Facsimile No.: 075-712-5161

III-1 Other applicant(s) or inventor(s)

III-1-1 Parties entered in this column are: Applicant and inventor

III-1-2 Applicant applicable to the country designated on the right: US only

III-1-4ja Name (Last, First): Shindo, Jiro

III-1-4en Shindo, Jiro

III-1-5ja Address: c/o K.K. Digital Publishing Japan
196-1 Kamigamohonzan, Kita-ku, Kyoto-shi, Kyoto 603-8047, Japan
III-1-5en c/o K.K. Digital Publishing Japan
196-1 Kamigamohonzan, Kita-ku, Kyoto-shi, Kyoto 603-8047, Japan
III-1-6 Nationality (Name of country): Japan JP
III-1-7 Address (Name of country): Japan JP

IV-1 Agent or assigned representative, Address to which report is made
The party below acts in the capacity indicated on in behalf of the applicant in the international organization: Agent
IV-1-1ja Name (Last, First): Umeda, Akihiko
IV-1-1en Umeda, Akihiko
IV-1-2ja Address: c/o Umeda & Co. No. 3 Seiko Building 7F
3-6-10 Akasaka, Minato-ku, Tokyo 107-0052, Japan
IV-1-2en c/o Umeda & Co. No. 3 Seiko Building 7F
3-6-10 Akasaka, Minato-ku, Tokyo 107-0052, Japan
IV-1-3 Telephone No.: 03-3560-8117
IV-1-4 Facsimile No.: 03-3560-8210
V Designation of countries
V-1 World patent (Enter other types of protection or handling in parentheses when so requested.):
EA: AM AZ BY KG KZ MD RU TJ TM and other signatory states of the Patent Cooperation Treaty with Eurasian Patent Treaty
EP: AT BE CH&LI CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE and other signatory states of the Patent Cooperation Treaty with European Patent Agreement
V-2 National patent (Enter other types of protection or handling in parentheses when so requested.): CN JP KR US
V-5 Declaration of confirmation on designation
Applicant designates all other Patent Cooperation Treaty contracting states according to the provisions of regulation 4.9 (b) in addition to the designation above. However, designation of the states indicated in column V-6 is excluded. Applicant declares that these additional designations are required to be confirmed, that those designations not confirmed within 15 months of the priority date are considered to have been withdrawn by the applicant once said period has expired.
V-6 States excluded from confirmation on designation: None
VI-1 Priority claimed based on previous national applications

VI-1-1 Previous Filing Date: August 27, 1999 (08.27. 1999)

VI-1-2 Previous Application No.: Patent Application No. Hei 11[1999]-283295

VI-1-3 Name of country: Japan JP

VI-2 Request for delivery of priority certificate

Transcripts of acceptance of those applications cited above that are indicated on the right should be sent by the accepting agency to the International Secretariat.

VII-1 International search agency (ISA) designated: Patent Office of Japan (ISA/JP)

VIII Reference	Number of pages	Electronic data attached
VIII-1 Application	3	
VIII-2 Specifications	10	
VIII-3 Claims	4	
VIII-4 Abstract	1	abst...txt
VIII-5 Figures	2	
VIII-7 Total	20	

Document attached	Attached	Electronic data attached
VIII-8 Statement of fees	✓	
VIII-9 Separate power of attorney with signature and seal	✓	

VIII-16 PCT-EASY disk Flexible disk

VIII-18 No. of figures to be presented with abstract

VIII-19 Language used for international application: Japanese

IX-1 Signature and seal of submitter

IX-1-1 Name (Last, First): Umeda, Akihiko [seal]

Column for use by Accepting Agency

10-1 Actual reception date of document submitted as international application

10-2 Figure

10-2-1 & 10-2-2 Lacking figure(s) received

10-3 Actual reception date (corrected date) of document or figure which completes the document submitted as international application and submitted subsequently within said period

10-4 Reception date within the required period for completion in accordance with Item 11 (2) of Patent Cooperation Treaty

10-5 International search agency designated by applicant: ISA/JP

10-6 Manuscript for investigation not sent to international search agency because search fee is not paid

Column for use by International Secretariat

11-1 Reception date of original record manuscript

[recurring header:] [pages 1-2 of 2]

International Application Form in accordance with Patent Cooperation Treaty

Original copy (for application) – Time and date printed August 28, 2000 (08.28. 2000) Monday 16 h. 24 min. 15 sec.

(This form does not constitute any part of international application and is not international application)

0 Column for use by accepting agency

0-1 International Filing No.

0-2 Stamp of date by accepting agency

0-4 Form-PCT/R0/101 (attachment)

This PCT fee statement

0-4-1 was prepared according to the right: PCT-EASY Version 2.91 (updated 07.01.2000)

0-9 Document symbol of applicant or agent: 12577

2 Applicant: K.K. Digital Publishing Japan

12	Calculation of prescribed fees		Amount/factor	Subtotal (JPY)
12-1	Handling charge	T	⇨	18,000
12-2	Investigation fee	S	⇨	72,000
12-3	International fees			
	Basic fee (Up to first 30 pages) b1		40,700	
12-4	Number of pages in excess of 30: 0			
12-5	Fee per page (X): 940			
12-6	Total fees b2: 0			
12-7	b1 + b2 =	B	40,700	
12-8	Designated fees:			
	Number of countries designated in international application: 6			
12-9	Number of designated fees to be paid (maximum of 8): 6			
12-10	Fee per 1 designation (X): 8,000			
12-11	Total designated fees D: 52,000			
12-12	Reduction in fees due to PCT-EASY R: –12,500			
12-13	Total international fees (B+D–R) I:		⇨	81,000
12-14	Priority certificate request fee			
	Number of request for priority certificate: 1			
12-15	Fee per 1 priority certificate (X): 1,400			
12-16	Total of priority certificate request fees P:		⇨	1,400

12-17 Total fees to be paid (T+S+I+P): 172,400

12-19 Method of payment: Transfer to bank account

Result of EASY check and reference made by applicant

13-2-2 Result of EASY check: Green?

Designated states: More designations can be made. (Following states remain undesignated:

AP:(GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW); OA:(BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG); AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, LI, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, KE, KG, KP, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW)

Please confirm them.

13-2-4 Result of EASY check: Yellow!

Priority: Priority requested 1:

It has been at least 12 months since the day priority was requested. Pleases confirm.

13-2-10 Result of EASY check: Green?

Column for use by accepting agency/International Secretariat: PCT-EASY used for preparing this application runs on Windows using non-English or a non-western-European language. Please compare application with electronic data carefully with respect to characters other than ASCII characters.

[pages 1–15]

Specifications

Image data distribution method and system, image data and recording medium

Technological field

The present invention pertains to technology for network distribution of a digitized image; particularly, to an image data distribution method and a system therefore as well as image data to be utilized therein.

Background of the technology

In general, since digital image data distributed via a network, such as the Internet, can be easily duplicated without impairing the picture quality, such data should be protected against illegal use; for example, against redistribution and/or duplication by unauthorized individuals. Thus, Japanese Kokai Patent Application No. Hei 9[1997]-191394, for example, discloses a method referred to as an electronic watermark or digital watermarking, which has been developed in order to embed copyright and source information in the image data to be distributed.

However, this type of electronic watermarking, which merely adds the copyright source, has the problem that even when illegal use occurs, the distribution route of the data, that is, when, to which clients, and under what conditions was the data distributed, could not be specified. Thus, for example, Japanese Kokai Patent Application No. 2000-50047 discloses a data distribution method in which information for designating the distribution destination is embedded in the image data. However, even with this data distribution method, because no information on which user is responsible is contained, the redistribution route of data is unlikely to be specified accurately.

Thus, the purpose of the present invention is to present an image data distribution method and a system therefor with which actual use of distributed image data by users can be found accurately, the redistribution route of the data can be specified easily in the event of an illegal use, and illegal use of the image data can be prevented or effectively curtailed.

Disclosure of the invention

The present invention concerns an image data distribution method characterized in that it contains a step in which image data distributed from the server side is unarchived to a memory on the client side, and user security data is then added to the unarchived image data in order to prevent illegal use of image data resulting from the distribution of image data from the server side to the client side via a network.

Accordingly, security data, that is, user or client identification data for the prevention of illegal use, can be added to the image data by the client who received the distributed image data, so that if the image data is used illegally, its redistribution route can be easily traced. Thus, an effective psychological restraint against the illegal use of image data can be achieved.

In a particular application example, a process in which the user security data is transmitted from the client side to the server side and a step in which said security data is stored in a storage device on the server side are included wherein security data added to given image data and the security data stored on the server side can be cross-referenced in the event of illegal use of the image, so that the redistribution route of the image data can be more accurately traced.

Preferably, the security data may be added to image data in the form of an electronic watermark.

More preferably, the security data can be added to the image data by selecting several pixels at non-adjacent positions locations among the pixels for the aforementioned image data unarchived to a memory and by increasing or decreasing the luminance level of the aforementioned pixels selected.

In addition, the present invention concerns an image data distribution method characterized in that it includes a step in which an instruction is given so that the aforementioned client can gain access to a security controller which performs authorization for image data distribution in response to a request made by the client, and a step in which an electronic key for unarchiving the image data is transmitted from the aforementioned security controller to the aforementioned client side in response to the authorization request for image data distribution from the aforementioned client side on the aforementioned server side in order to prevent illegal use of image data resulting from the distribution of image data from the server side to client side via a network.

When distribution destinations are verified in advance in this manner, the image data can be prevented from being distributed to unauthorized users or clients.

In a particular application example, a step for storing the communication status on the client side is provided. Accordingly, said distribution destination can be easily identified on the server side after the distribution of image data, so that in the event of illegal use, its redistribution route can be easily traced.

In another application example, it is desirable that a security controller be provided separately from the server used for image data distribution, and the client side is instructed to gain access to the security controller using a IP address given to it.

In another application example of the present invention, a storage medium containing software for the execution of said image data distribution method is presented on the client side or the server side.

In yet another application example of the present invention, the image data distribution method is characterized as a method for distributing image data from a server to clients and comprises a step in which an instruction for the aforementioned client side to gain access to a security controller is given from the server side in response to a request for image data by the client, a step in which the aforementioned client gains access to the aforementioned security controller in order to be authorized for image data distribution, a step in which image data corresponding to the aforementioned request is transmitted from the aforementioned server side to the aforementioned client side, a step in which an image key for opening the aforementioned image data is transmitted from the aforementioned server side to the aforementioned client side, a step in which the aforementioned image data is unarchived using the aforementioned image key on the aforementioned client side, and user security data is added to said image data, and a step in which the image data to which the aforementioned security data has been added is output.

When so configured, because distribution destinations can be verified in advance in order to prevent image data from being distributed to unauthorized users or clients, and a client who actually received the image data can add security data, that is, user or client identification data for the prevention of illegal use, to the image data, the redistribution route in the event of illegal use of the image data can be easily traced. Therefore, not only can the illegal use of image data be effectively prevented, but also there results a strong psychological restraint against the illegal use of image data.

In a particular application example, because a step in which the aforementioned security data is transmitted to the server side and a step in which said security data is stored by the server are further provided, in the case of illegal use of image data, the security data that has been added to the image data and the security data stored by the server can be cross-referenced in order to trace and specify the redistribution route of the image data more accurately.

In another application example, because the server is further provided with a step in which communication status with the client is stored in a log file, a client or user culpable of illegal use can be specified more accurately and easily.

In addition, in a particular application example, it is desirable that a security controller be provided separately from the server used for image data distribution, and access to the security controller is instructed by giving an IP address to the client side.

In another application example, image data transmitted from the server side is compressed, so that the security data can be added after said image data is unarchived on the client side.

In addition, it is desirable that the security data be added to the image data in the form of an electronic watermark.

In a specific application example, the security data can be added to the image data by selecting several pixels at non-adjacent positions locations among the pixels for the image data unarchived using the aforementioned image key and by increasing or decreasing the luminance level of the aforementioned selected pixels.

The date and time of the distribution of the image data, user ID, and the serial number of the client storage device storing the image data or the IP address of the client may be included in the security data. When they are utilized, the redistribution route after the distribution of the image data can be easily traced.

The present invention also provides an image data distribution system that is characterized in that it is equipped with an image file server having an image file database containing image files, a security control server having a user database containing registration data on respective users and an image key database containing image keys for unarchiving respective image files to clients, and a network for connecting the image file server, the security control server, and the clients; wherein,

the image file server has a function of instructing a client to gain access to the security control server in response to a request from said client for image data and a function of transmitting the image data requested to the client,

the client has a function of gaining access to the security control server to request for user authorization in order to obtain the image data,

the security control server has functions of verifying via the user database, the user in response to the client's request for authorization and of then transmitting the image key to the requested image data from the image key database, and

the client is further provided with functions for unarchiving the image data received using the image key and for adding user security data to said image data.

When so configured, distribution destinations can be authorized in advance in order to prevent image data from being distributed to unauthorized users or clients, and the redistribution route of image data can be specified easily, since security data, that is, user or client identification data, is added to the image data by the client who received the image data, so that an image data distribution method with which illegal use of image data can be prevented and psychologically discouraged more reliably than ever can be realized.

In a particular application example, because the client has also the function of transmitting the security data to the security control server, and the security control server also has the function of storing the security data, the security data in the image data and the one stored in the security control server can be cross-referenced at a later time.

In another application example, because the security control server has a log file to store the communication status with a client, the image data distribution status can be ascertained more accurately.

It is desirable that the image file server give the instruction for gaining access to the security control server through the provision of the IP address.

In a particular application example, image data transmitted from the image file server is compressed, so that the client unarchives the image data received before adding the security data.

It is desirable that the client add the security data to the image data in the form of an electronic watermark.

In addition, it is convenient if the security data contain the date and time of the distribution of the image data, user ID, and the serial number of the client's storage device storing the image data or the IP address of the client when specifying the redistribution route of the image data.

Furthermore, the present invention also provides image data with embedded user information by increasing or decreasing the luminance levels of several selected pixels placed at discrete locations on a map of pixel data represented by dots.

Brief description of the figures

Figure 1 is a diagram showing the outlined configuration of a preferred application example of the image data distribution system in accordance with the present invention.

Figure 2 is a flowchart showing the process of image data distribution in the image data distribution system in Figure 1.

Preferred embodiment of the invention

Figure 1 shows the outline of a system configuration on the Internet as a preferred application example of the image distribution system in accordance with the present invention. The image distribution system in the present application example is configured with multiple clients (2) connectable via a network environment, such as the Internet (1), an image filer server (3), and a security control server (4). The client (2) is a computer provided with functions for transmitting a request specifying a desired image to the image file server (3) using WWW browser on the Internet (1) in order to receive digital image data from said server and for regenerating the image.

The image file server (3) is made of a computer for transmitting image data in response to the request from the client (2) on the Internet and provided with a file database (5) containing image files and a log file (6) for storing communication status with the client (2). Furthermore, the image file server (3) has the function of transmitting an IP address for the security control

server (4) in response to the request for image data from the client (2) in order to instruct the client (2) to gain access to the security control server and the function of transmitting the requested image data from the image file database (5) to the client.

In the present application example, compressed hierarchized image files having a data structure in which digitized image data is hierarchized once according to the significance of the information (for example, luminance level or changes in luminance level) the respective pixels have and then restructured are stored in the image file database (5). These hierarchized image files can be generated using, for example, the image compression method described in the specifications of International Patent Application No. PCT/JP00/04472 by the inventor of the present application. Said hierarchized image files comprise information on the positions and the luminance levels of respective pixels. Because the images differ in terms of quality, that is, resolution, depending on their ranking and size, the client can specify the image quality when requesting image data.

The security control server (4) has a user database (7) containing the contents of the registrations of users who are allowed to utilize the image files in the image file database (5), an image key database (8) containing the necessary image keys for unarchiving the aforementioned image files, and a log file (9) for storing communication statuses with clients (2). Respective users and their identification data are classified into several groups and registered in the user database (7) of the present application example. Each group is granted certain rights, so that they select the corresponding quality, that is, resolution, and size.

The client (2) can gain access to the security control server using the IP address for the security control server (4) received from the image file server (3) in order to request for authorization to acquire the image data. The security control server (4) verifies the user through database (7) in response to said authorization request and transmits an image key peculiar to the image data requested from the image key database (8).

The client (2) is also able to unarchive the image data received from the image file server (3) into the memory using the aforementioned image key and to add user security data to said image data. Said security data contains identification data on the client or user, such as the date and time of the distribution of the image data, user ID, serial number of the storage device, for example, a hard disk drive, to which the image data was downloaded, IP address of the client (2), which are useful for tracing the redistribution route in the event of illegal use.

Next, a preferred application example of the image distribution method in accordance with the present invention will be explained using Figure 2. First, the client (2) activates a general-purpose or WWW-dedicated browser in order to get connected to the image file server (3) via the Internet. Once the client (2) transmits a request specifying the name and the quality of the desired image file (step S1), the image file server (3) returns an IP address for the security

control server (4) (step S2). The client (2) gains access to the security control server (4) using said IP address in order to request for authorization to acquire the image data (step S3). User ID, client's IP address, and serial number of the hard disk drive as data peculiar to the client are utilized for said authorization.

The security control server (4) verifies registered data, such as user ID, in reference to the user database (7) before granting authorization (step S4). Then, an image key peculiar to the image data requested is obtained from the image key database (8) and transmitted to the client (2) (step S5), and the status of this communication is stored in the log file at the same time (9) (step S6). On the other hand, the image filer server (3) obtains the image data requested from the image file database (5) and transmits it to the client (2) (step S7). Similarly, the image file server (3) also stores the communication status with the client (2) in the log file (6).

The client (2) opens and decompresses the image data received from the image file server (3) using the image key received from the security control server (4) and unarchives it to memory as a pixel data map of the respective pixels constituting the image (step S8). Then, the security data is encoded and added to the unarchived image data (step S9). In general, the addition of security data is achieved using a so-called electronic watermark. In the present application example, an electronic watermark can be inserted by selecting several pixels placed at non-adjacent positions locations among the pixels for the aforementioned unarchived image data and increasing or decreasing the luminance levels of the aforementioned pixels. The positions of the aforementioned pixels can be selected in advance, and they can be also changed depending on the contents of the image.

The image data to which the security data has been added in said manner is output (step S10) and can be utilized in a variety of ways; for example, displayed directly on the client's display, stored in a storage device, such as a hard disk drive, or other storage media; or transmitted on-line to another apparatus. At the same time, the client (2) transmits the aforementioned security data to the security control server (4) (step S11), and the security control server (4) stores it in the log file (9) (step S12).

As a result, because a record on the distribution of the image data is kept in the security control server (4), in the event of subsequent illegal use of the image data, its redistribution route can be easily specified by cross-referencing the security data embedded in the image data. In addition, in the present application example, because the image file server (3) and the security control server (4) are provided separately, security data transmitted from clients can be managed once the address of the security control server (4) is preset on the network even when the image file server (3) is set to an arbitrary address as needed, that is, when the image file database (5) is set to an arbitrary address.

In another application example of the present invention, the image file server (3) and the security control server (4) can be integrated in order to use a single server for the configuration. In this case, access to the security control server (4) and use of the image key can be omitted. That is, the client (2) first requests authorization from the server for image distribution; and after the server has granted authorization in reference to the user database (7) in response to said request, the client (2) requests distribution of the desired image in order to have the image transmitted. Needless to say, in this case, too, after the client has opened the image data and unarchived it into the memory, security data is added to the image data in the same manner as that in the aforementioned application example and transmitted to the server, and the server stores it into the log file.

Moreover, in yet another application example, the IP address for the security control server (4) can be added to the image data distributed from the image file server (3) in advance. In this case, upon receiving an image data distribution request from the client (2), the image file server (3) transmits the image data requested. The client (2) reads the IP address from the image data received and gains access to the security control server (4) in order to request authorization. Once the security control server (4) completes authorization and transmits the image key, the client (2) is able to open the image data using said image key.

A preferred application example of the present invention was explained in detail above. As is clear to an expert in the field, the present invention can be implemented with various kinds of changes and modifications to the aforementioned application example without exceeding the scope of the invention. For example, the present invention can also be applied to a network other than the Internet in the same manner.

Claims

1. An image data distribution method characterized in that it contains a step in which image data distributed from the server side is unarchived into a memory on the client side, and user security data is then added to the unarchived image data in order to prevent illegal use of image data resulting from the distribution of image data from the server side to the client side via a network.

2. The image data distribution method of Claim 1, characterized as further containing a process in which the aforementioned user security data is transmitted from the aforementioned client side to the aforementioned server side and a step in which the aforementioned security data is stored in a storage device on the aforementioned server side.

3. The image data distribution method of Claim 1 or 2, characterized in that the aforementioned security data is added to the aforementioned image data in the form of an electronic watermark.

4. The image data distribution method of one of Claims 1 through 3, characterized in that the aforementioned security data is added to the aforementioned image data by selecting several pixels in non-adjacent positions locations from the pixels of the aforementioned unarchived image data and by increasing or decreasing the luminance level of the aforementioned selected pixels.

5. An image data distribution method characterized in that it includes a step on the server side in which an instruction is given for the aforementioned client side to gain access to a security controller which authorizes distribution of image data in response to a request made by the client, and a step on the server side in which an electronic key for unarchiving the image data is transmitted from the aforementioned security controller to the aforementioned client side in response to the authorization request for image data distribution from the aforementioned client side in order to prevent illegal use of image data resulting from the distribution of image data from the server side to the client side via a network.

6. The image data distribution method of Claim 5, characterized as further containing a step for storing the client communication status.

7. The image data distribution method of Claims 5 or 6, characterized in that access to the aforementioned security controller is instructed through the provision of IP address for the aforementioned security controller.

8. A storage medium containing software for the execution of the image data distribution method of one of Claims 1 through 3 and 5 through 7.

9. An image data distribution method characterized in that it is a method for distributing image data from a server to a client comprising

a step in which an instruction for the aforementioned client side to gain access to a security controller is given from the server side in response to a request for an image data by the client side,

a step in which the aforementioned client side gains access to the aforementioned security controller in order to be authorized to receive image data,

a step in which image data corresponding to the aforementioned request is transmitted from the aforementioned server side to the aforementioned client side,

a step in which an image key for opening the aforementioned image date is transmitted from the aforementioned server side to the aforementioned client side,

a step in which the aforementioned image data is unarchived using the aforementioned image key on the aforementioned client side, and user security data is added to said image data, and a step in which the image data added with the aforementioned security data is output.

10. The image data distribution method of Claim 9, characterized in that it also contains a step in which the aforementioned security data is transmitted to the aforementioned server side and a step in which said security data is stored by the aforementioned server side.

11. The image data distribution method of Claim 9 or 10, characterized in that the aforementioned server side is further provided with a step in which communication status with the client side is stored in a log file.

12. The image data distribution method of one of Claims 9 through 11, characterized in that access to the aforementioned security controller is instructed through the provision of IP address for the aforementioned security controller.

13. The image data distribution method of one of Claims 9 through 12, characterized in that the aforementioned image data transmitted from the server side is compressed, so that the aforementioned security data is added after said image data is unarchived upon the request from the aforementioned client.

14. The image data distribution method of one of Claims 9 through 13, characterized in that the aforementioned security data is added to the aforementioned image data in the form of an electronic watermark.

15. The image data distribution method of one of Claims 9 through 14, characterized in that the aforementioned security data is added to the aforementioned image data by selecting several pixels placed at non-adjacent positions locations among the pixels for the aforementioned image data unarchived using the aforementioned image key and by increasing or decreasing the luminance level of the aforementioned pixels selected.

16. The image data distribution method of one of Claims 9 through 15 characterized in that the date and time of the distribution of the aforementioned image data, user ID, and the serial number of the aforementioned client's storage device storing the aforementioned image data or the IP address of the aforementioned client are included in the aforementioned security data.

17. An image data distribution system characterized in that it is equipped with an image file server having an image file database containing image files,

a security control server having a user database containing registration data on the respective users and an image key database containing image keys for unarchiving the aforementioned respective image files,

clients, and

a network for connecting the aforementioned image file server, the aforementioned security control server, and the aforementioned clients; wherein,

the aforementioned image file server has the function of instructing the client to gain access to the aforementioned security control server in response to a request from the

aforementioned client for image data and a function of transmitting the image data requested to the aforementioned client,

the aforementioned client has a function of gaining access to the aforementioned security control server to request user authorization to obtain the aforementioned image data,

the aforementioned security control server has functions of verifying, via the aforementioned user database, the user authorization in response to the aforementioned client's request for authorization and of then transmitting the image key to the aforementioned requested image data from the requested image key database, and

the aforementioned client is further provided with functions for unarchiving the aforementioned image data received using the aforementioned image key and for adding the aforementioned user security data to the aforementioned image data.

18. The image data distribution system of Claim 17 characterized in that the aforementioned client has also a function of transmitting the aforementioned security data to the aforementioned security control server, and that the aforementioned security control server also has a function of storing the aforementioned security data.

19. The image data distribution system of Claim 17 or 18, characterized in that the aforementioned security control server has a log file to store communication statuses with the aforementioned clients.

20. The image data distribution system of one of Claims 17 through 19, characterized in that the aforementioned image file server gives an instruction to gain access to the aforementioned security control server through the provision of the IP address.

21. The image data distribution system of one of Claims 17 through 20, characterized in that the aforementioned image data transmitted from the aforementioned image file server is compressed, so that the aforementioned client unarchives the aforementioned received image data before adding the aforementioned security data.

22. The image data distribution system of one of Claims 17 through 21, characterized in that the aforementioned client has the function of adding the aforementioned security data to the aforementioned image data in the form of an electronic watermark.

23. The image data distribution system of one of Claims 17 through 22, characterized in that the aforementioned security data contains the date and time of the distribution of the aforementioned image data, user ID, and the serial number of the aforementioned client's storage device storing the aforementioned image data or the IP address of the aforementioned client.

24. Image data characterized in that user information is embedded by increasing or decreasing the luminance levels of several selected pixels at non-adjacent positions within a map made up of pixel data in the form of dots.

Abstract

An image distribution system is configured with multiple clients 2 connectable via a network environment, such as Internet 1; image file server 3 having image file database 5 containing image files and log file 6; user database 7; and security control server 4 having image key database 8 and log file 9. Image data from the image file server can be opened once the client who made the image data request gains access to the security control server using an IP address obtained from the image file server, is granted authorization, and obtains an image key. The client encodes security data, such as the date and time of the distribution of the image data, user ID, serial number of hard disk drive, and client's IP address, in order to embed it in the image data unarchived into its memory in the form of an electronic watermark and transmits the security data to the security control server in order to store it in the log file at the same time.

CLAIMS

1. An image data distribution method comprising:

storing image data distributed from the server side into a memory on the client system side; and

adding user security data to the stored image data in order to prevent illegal use of image data resulting from the distribution of image data from the server side to the client system side via a network.

2. The image data distribution method of Claim 1, further comprising:

transmitting user security data from the client system side to the server side; and

storing the security data in a storage device on the server side.

3. The image data distribution method of Claim 1, wherein the security data is added to the image data in the form of an electronic watermark.

4. The image data distribution method of Claim 1, wherein the security data is added to the image as an electronic window.

5. The image data distribution method of Claim 1, wherein security data is added to the image data by selecting several pixels in non-adjacent positions locations from the pixels of the unarchived image data and by increasing or decreasing the luminance level of the selected pixels.

6. An image data distribution method comprising:

giving an instruction for the client system side to gain access to a security controller which authorizes distribution of image data in response to a request made by the client system; and

transmitting an electronic key for unarchiving the image data from the security controller to the client system side in response to the authorization request for image data distribution from the client system side in order to prevent illegal use of image data resulting

from the distribution of image data from the server side to the client system side via a network.

7. The image data distribution method of Claim 5, wherein image data have image files of varying image quality; and the request from the above-mentioned client includes a designation of image quality.

8. The image data distribution method of Claim 7, wherein the said image data have image files with a data structure which is made hierarchical by the image quality.

9. The image data distribution method data of Claim 7, wherein said image quality is the resolution or size of the images.

10. The image data distribution method of Claim 6, further comprising storing the client system communication status.

11. The image data distribution method of Claim 6, wherein access to the security controller is instructed through the provision of IP address for the security controller.

12. A storage medium containing software that enables a program to execute, the storage medium comprising:

code for storing image data distributed from the server side into a memory on the client system side; and

code for adding user security data to the stored image data in order to prevent illegal use of image data resulting from the distribution of image data from the server side to the client system side via a network.

13. An image data distribution method for distributing image data from a server to a client system comprising:

giving an instruction from the server side for the client system side to gain access to a security controller in response to a request for an image data by the client system side;

providing the client system side access to the security controller in order to be authorized to receive image data;

transmitting image data corresponding to the request from the server side to the client system side;

transmitting an image key for opening the image date from the server side to the client system side;

unarchiving image data using the image key on the client system side;

adding user security data to said image data; and

outputting the image data having the added security data.

14. The image data distribution method of Claim 13 further comprising:

transmitting the security data to the server side; and

storing said security data at the server side.

15. The image data distribution method of Claim 13 further comprising storing the communication status with the client system side in a log file.

16. The image data distribution method of Claim 13, wherein access to the security controller is instructed through the provision of IP address for the security controller.

17. The image data distribution method of Claim 13, wherein the image data transmitted from the server side is compressed, so that the security data is added after said image data is unarchived upon the request from the client system.

18. The image data distribution method of Claim 13, wherein the security data is added to the image data in the form of an electronic watermark.

19. The image data distribution method of Claim 13, wherein the security data is added to the image data by selecting several pixels placed at discontinuous positions locations among the pixels for the image data unarchived using the image key and by increasing or decreasing the luminance level of the pixels selected.

20. The image data distribution method of Claim 13, wherein the date and time of the distribution of the image data, user ID, and the serial number of the client system's storage device storing the image data or the IP address of the client system are included in the security data.

21. The image data distribution method of Claim 13, further comprising:

transmitting image data having image files of varying image quality; and

requesting from said client a designation of image quality.

22. The image data distribution method of Claim 21, wherein said image data have image files with a data structure which is made hierarchical by the image quality.

23. The image data distribution method of Claim 21, wherein said image quality is the resolution or size of the images.

24. An image data distribution system comprising:

an image file server having an image file database containing image files;

a security control server having a user database containing registration data on the respective users and an image key database containing image keys for unarchiving the respective image files;

a network for connecting the image file server, the security control server, and to client systems; wherein,

the image file server has the function of instructing the client system to gain access to the security control server in response to a request from the client system for image data and a function of transmitting the image data requested to the client system;

the client system has a function of gaining access to the security control server to request user authorization to obtain the image data;

the security control server has functions of verifying, via the user database, the user authorization in response to the client system's request for authorization and of then transmitting the image key to the requested image data from the requested image key database; and

the client system is further provided with functions for unarchiving the image data received using the image key and for adding the user security data to the image data.

25. The image data distribution system of Claim 24, wherein said image data have image files of varying image quality; and the request from the above-mentioned client includes a designation of image quality.

26. The image data distribution system of Claim 25, wherein the image data have image files with a data structure which is made hierarchical by the image quality.

27. The image data distribution system of Claim 25, wherein said image quality is the resolution or size of the images.

28. The image data distribution system of Claim 24, wherein the client system has also a function of transmitting the security data to the security control server, and that the security control server also has a function of storing the security data.

29. The image data distribution system of Claim 24, wherein the security control server has a log file to store communication statuses with the client systems.

30. The image data distribution system of Claim 24 wherein the image file server gives an instruction to gain access to the security control server through the provision of the IP address.

31. The image data distribution system of Claim 24 wherein the image data transmitted from the image file server is compressed, so that the client system unarchives the received image data before adding the security data.

32. The image data distribution system of Claim 24 wherein the security data contains the date and time of the distribution of the image data, user ID, and the serial

number of the client system's storage device storing the image data or the IP address of the client system.

33. Image data having user information embedded therein by increasing or decreasing the luminance levels of several selected pixels positions which are not continuous within a map made up of pixel data in the form of dots.